secmaker

PRODUKTBLAD

10 steg mot en lösenordsfri inloggning

10 steg mot en bra inloggning

Att komma igång med förändringar i en organisation kan vara nog så krävande. Byte av lösning för bättre och säkrare inloggning med hjälp av PKI och certifikat är inget undantag. SecMaker har medverkat i 100-tals projekt, några av dem bland de största i världen, under mer än 15 år. Vi vet att om du följer dessa 10 steg ökar dina chanser att lyckas med projektet markant.

Utgångspunkten nedan är att du har en Microsoft Server miljö och valt PKI som informationssäkerhetsmetod, det vill säga certifikatbaserad inloggning till dator, domän, webb och applikationer.

1 Inventera behovet och avgränsa

Så fort man börjar få en överblick av säkerhetsbrister och behov av åtgärder skenar åtgärdslistan och man lockas att skjuta besluten framför sig. En annan vanlig reaktion är att man tar fram massor av processer, styrdokument och beslutsunderlag. Ofta i samarbete med en informationssäkerhetskonsult. Det är inget fel att göra det men när teori och praktik går hand i hand kommer resultatet snabbare. Annars blir det som att köpa ett par löparskor och sedan sitta i flera månaders möten med sin PT om hur man ska lägga upp träningen.

Avgränsa projektet till att inledningsvis skydda inloggningen till domän, VPN och de mest skyddsvärda målsystemen. Ta sedan nästa, nästa och nästa steg. Ett i taget. Det som är så bra med certifikat och PKI är att man kan använda grundinvesteringen för väldigt många behov utan extra kostnad.

2 Välj trust level

Låt oss säga att e-legitimation är den högsta tillitsnivån på ett certifikat. Det ska vara oavvisligt och inte gå att förfalska. Då krävs motsvarande processer som vid utgivning av pass eller bankkort. Den lägsta tillitsnivån på ett certifikat är när en person ”Jocke på IT-avdelningen” får förtroendet att helt på egen hand ge ut, spärra och förnya organisationens digitala identiteter. Hans chef vet inte om ”Jocke” har ett förflutet i kyrkokören eller kriminellt gäng.

Beslutet om trust level går att krångla till oändligt. Att planera certifikathierarkin är ändå en av de viktigaste aspekterna i PKI-designen eftersom det kommer ha direkt påverkan på hur dina certifikat valideras och används av PKI-aktiverade målsystem.

Behovet styr men i ett vanligt företag som är verksam under vanliga lagar är en medelväg vanlig. Man har då en dokumenterad policy kring utfärdande och riskhantering.

3 Utse organisation och ansvarig

Ett vanligt fel är att IT-avdelningen utser en eller flera personer som redan har fullt upp att sköta införandet av säker tvåfaktorsautentisering. Personen ifråga är duktig och sugen på nya spännande utmaningar men glömmer att befintliga arbetsuppgifter tar sin tid. Alla dagar i veckan. Året runt.

Utse medarbetare som har tiden att genomföra förändringen. Det kostar i början men betalar sig snabbt i form av enklare administration och minskade risker när projektet är genomfört. Utgivningsprocess, hantering av reservkort och spärrning av kort/certifikat är viktiga frågor för lösningens trovärdighet och framgång. Inte minst i decentraliserade organisationer med arbetplatser på flera olika orter är dessa frågor helt avgörande för resultatet.

4 Välj bärare

Vad ska bära ditt certifikat? Ska det ligga lagrat på datorn (virtual smartcard), på mobiltelefonen, ska vi använda säkerhetsnycklar eller ska vi använda smartkort som bärare? Det finns för- och nackdelar med alla bärare. Det finns ingen inloggningslösning som passar alla behov. När du väljer bärare och kortläsare måste du kontrollera att inloggningen är snabb och fungerar som utlovat. Användarna gillar inte om deras inloggning blir långsammare än tidigare. Här gör kunderna ibland fel val, till exempel för att snåla in lite eller helt enkelt för att man låter sig luras av glada säljare.

Valet av manageringsverktyg är avgörande. Microsoft CA är en robust och bra certifikatutfärdare som ingår i Microsoft Server. Men att administrera utgivning av certifikat via Microsofts manageringskonsol är mycket tidskrävande och krångligt. Köp ett vettigt livscykelhanteringssystem som har bra referenser och går att få utbildning på.

5 Systemdesign

En stor fördel med PKI och certifikat är att det kan integreras mot befintliga system. Flera vägval påverkar dock användarupplevelsen. Om man glömmer bort dessa kan lösningen bli onödigt krånglig. Ibland så krånglig att det motverkar syftet med projektet.

Vad ska hända när användaren drar ut sitt smartkort ur kortläsaren? Ska datorn och applikationerna fortsätta vara påloggade? Ska arbetsstationen låsas så att arbetet är skyddat? Ska en annan användare kunna återuppta sin inloggning på en delad dator bara genom att växla kort? Hur snabbt sker detta?

Man kan konfigurera på många olika sätt samtidigt som beroenden av bakomliggande IT-infrastruktur också spelar stor roll för hur lösningen kan byggas. Vägvalen blir snabbt avgörande för användarens mottagande av den nya säkerhetslösningen.

6 Utbildning

Dina administratörer och projektägare måste lära sig förstå produkterna, hur de kan konfigureras, administreras, supporteras och vilka valmöjligheter som finns.

Använd erfarna rådgivare i projektet, personer som deltagit i liknande projekt och vet vad det handlar om. Produktleverantörer ger ofta frikostig hjälp och rådgivning för att få sälja sina produkter. Konsulter vill ge dig hjälp och rådgivning för att sälja sina konsulttimmar. Använd gärna en mix av båda för att få bästa effekt och för att skaffa dig en egen uppfattning.

7 POC, pilot och utvärdering

Att bygga en PKI hierarki by-the-book i en organisation med 500 användare är inte mycket mindre tidskrävande än att göra det för 10 000 användare. Det går att sätta upp sakerna enkelt och klicka next-next-next i installationswizarden. Men då måste allt göras om när ni har utvärderat lösningen och fattat beslut om att gå vidare. Ha med detta i beräkningen när du anlitar en specialist. Se specialistinsatsen som en framtida investering. Vi har medverkat i projekt som än idag fungerar alldeles utmärkt efter 10 år. Utslaget blir den initiala kostnaden då mycket låg.

Proof-Of-Concept och piloter är vanliga önskemål från våra kunder. Givetvis en bra utvärderingsform säger vi. Dock ser vi ofta att projekten börjar glida redan här eftersom det är datorvana användare med adminkonton på IT-avdelningen som är föremål för piloten. Ärligt – denna grupp ska ha smartkortkrav på sina adminkonton men har väldigt sällan det. Dom gör precis som dom vill och är ett dåligt underlag för utvärdering. Utse vanliga användare till att utvärdera lösningen och var noga med att följa upp användarnas reaktioner. Genom att utbilda dessa och konfigurera ihop lösningen går det mesta att få riktigt bra.

8 Ta steget

Det finns två effektiva sätt att påverka människor att förändra sitt beteende. Det ena är att tillföra kundnytta och det andra sättet är att tvinga dem. Ett lyckat PKI-projekt kombinerar båda. Kundnyttan kan till exempel ligga i singelinloggning och snabbhet. Ett vårdbiträde som har tio olika system att logga in i som kräver olika, krångliga lösenord som byts var tredje månad vittnar ofta om att en vettigt ihopskruvad smartkortlösning gör hennes vardag mycket enklare och samtidigt säkrare.

Det andra sättet att påverka människor att acceptera den nya inloggningslösningen är naturligtvis att stänga av möjligheten att logga in med lösenord. Windowspolicyn Smart card require gör att användaren bara kan logga in med sitt kort. Detta hårda grepp mottas ibland med stor frustration och användaren hittar på skäl till varför just hon ska undantas från kontoinställningen.

Har vi byggt vår inloggningslösning bra så ska detta inte kunna hända. Faktum är att vi ofta sett hur mycket stora organisationer med över 10 000 medarbetare på mindre än en vecka fått med sig alla användare till den nya lösningen. Den veckan är ofta mycket intensiv för helpdesken men veckan därpå är trycket på helpdesk mycket reducerat. När du läser det här så tror du kanske inte att det går att genomföra förändringen på en vecka? Jo det går men då måste vi först ha snickrat på rutinerna tillsammans ett tag och utbildat personalen.

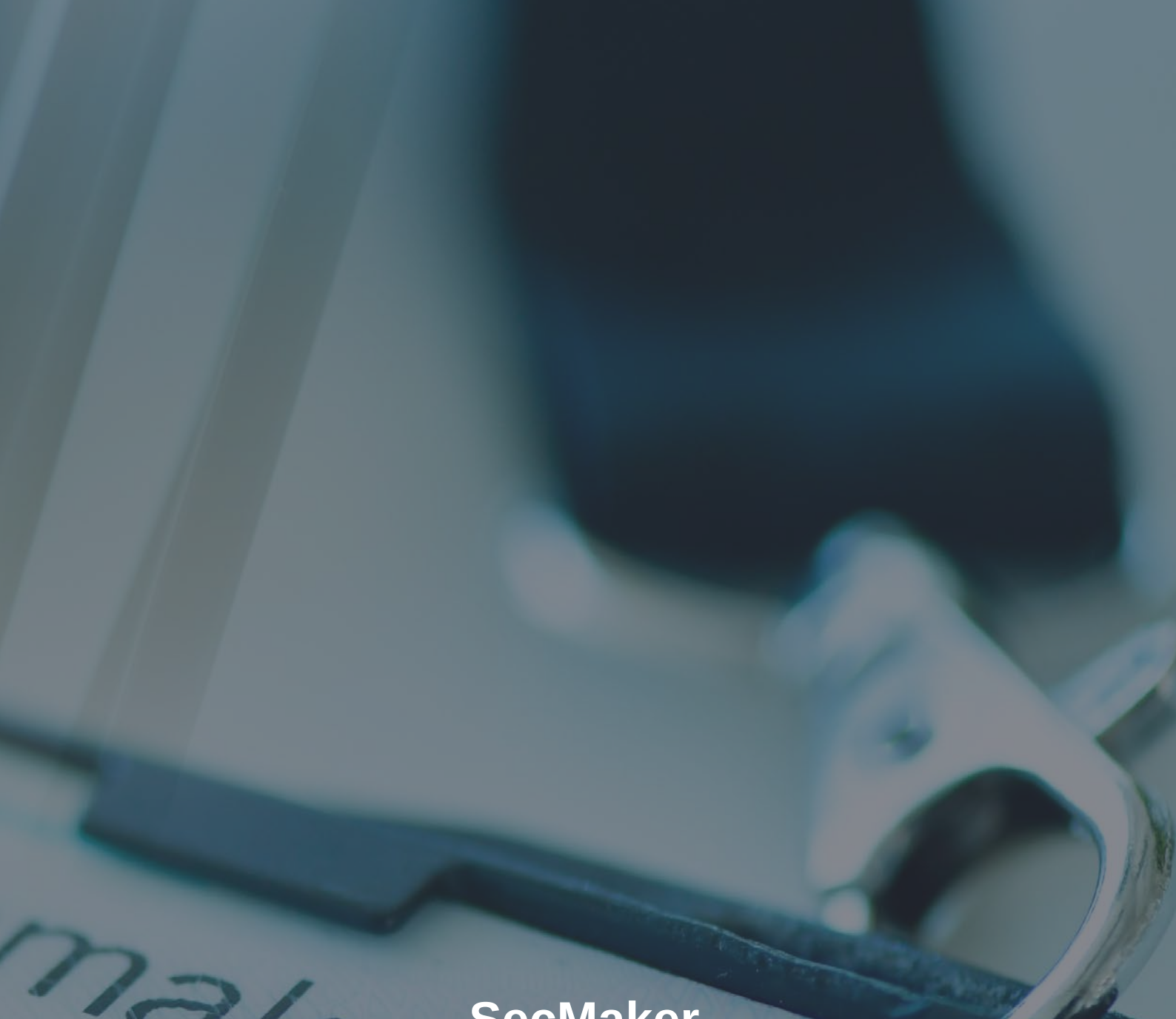
9 Beredskap

Det dyker alltid upp smarta personer som ringer helpdesk med alla möjliga argument mot den nya lösningen. Vi anser att många IT-avdelningar viker sig och börjar darra inför trycket från användarna. Finns det en policy så måste vi ta ansvar för den.

I beredskapen är utbildning den viktigaste ingrediensen och många gånger den viktigaste motivationsfaktorn. Medarbetarna måste känna att det ger organisationen status att vara säkerhetsmedveten. Då ökar motivationen.

10 Sist men inte minst

Den här artikeln gör inte anspråk på att vara heltäckande. Alla förstår att ett smartkort är säkrare än ett lösenord som kan hackas, kopieras eller vara inloggad hela dagen. I detaljerna bor djävulen. Vrider vi på frågeställningarna från alla synvinklar kan den flexibla, globalt standardiserade IT-säkerhetsmetoden PKI växa till ett monster. Våra produkter och lösningar syftar till att ge de allra bästa förutsättningarna att komma igång. Och sedan utveckla användningen i oändlighet.



SecMaker – med drivkraften att göra skillnad

Risken för identitetsstölder och nätbedrägerier växer snabbt. Inte minst för företagare som utsätts för virus, dataintrång, id-kapning, stulna lösenord och utpressningsprogram. I många fall kan konsekvenserna för verksamheten vara förödande. Men det går att öka säkerheten med enkla metoder, Secmaker hjälper dig att minska riskerna. Vi är Nordens ledande leverantör av certifikatbaserade säkerhetslösningar för företag, myndigheter och organisationer. Vi skyddar och säkerställer information, system och datatrafik hos över 1,5 miljoner nöjda användare.

Vill du veta mer?

Besök **www.secmaker.com** för mer information om våra lösningar. För fördjupad information eller en utvärderingslicens, kontakta oss på SecMaker via e-post **info@secmaker.com** eller telefon **08-601 23 00**.

secmaker

SecMaker AB
Uddvägen 7 | 131 54 Nacka
08-601 23 00 | info@secmaker.com

www.secmaker.com